



MSFC Public Key Infrastructure (PKI)

Protecting Your Data with Entrust



Lisa Hall
WILL Technology, Inc.
October 15, 2008



What is Public Key Infrastructure?



A system that manages electronic/digital keys used to lock and unlock computer data. (SBU, PAI, and PII)

The primary purpose is to enable you to share your data with other people in a secure manner.

The primary uses at MSFC are for digitally signing email/forms and file/email encryption.



Encrypting, Signing and Verifying

E-business requires confidentiality of sensitive information and authentication of the individual involved



Encrypt files, folders, e-mail messages and their attachments

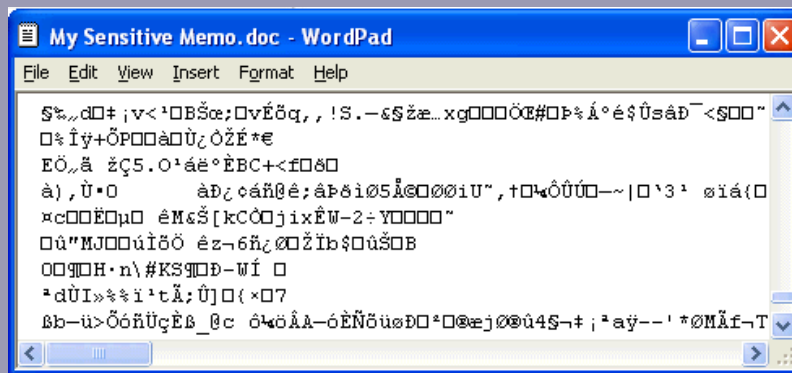


Digitally sign and authenticate files and electronic transactions



What is Encryption?

To encrypt a file is to render the file completely unreadable. No one, including you, can read the file until it is decrypted. Only you and recipients whom you authorize can decrypt the file.

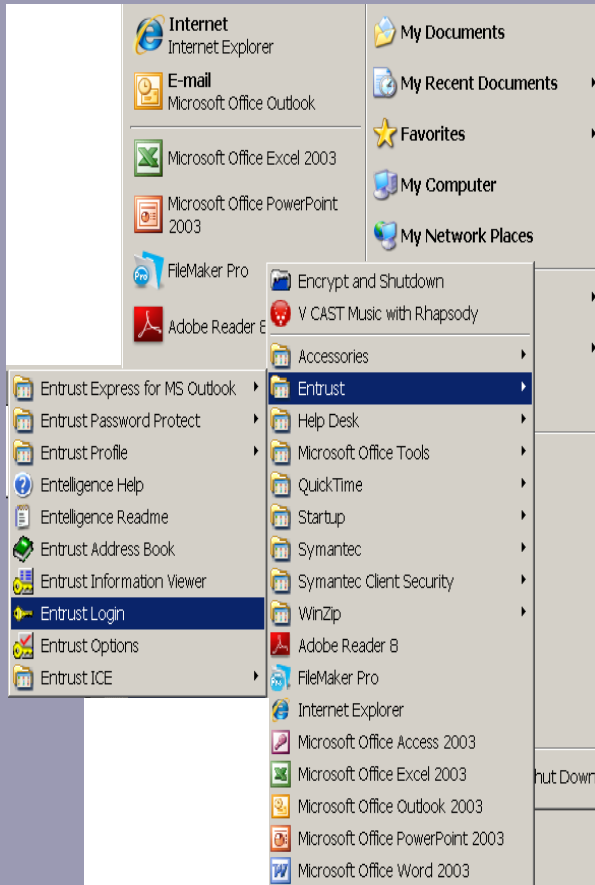


You and others whom you authorize to read your files simply double-click the file and it is restored to it's original form.

To open the file you will need to login to Entrust.



Entrust Login



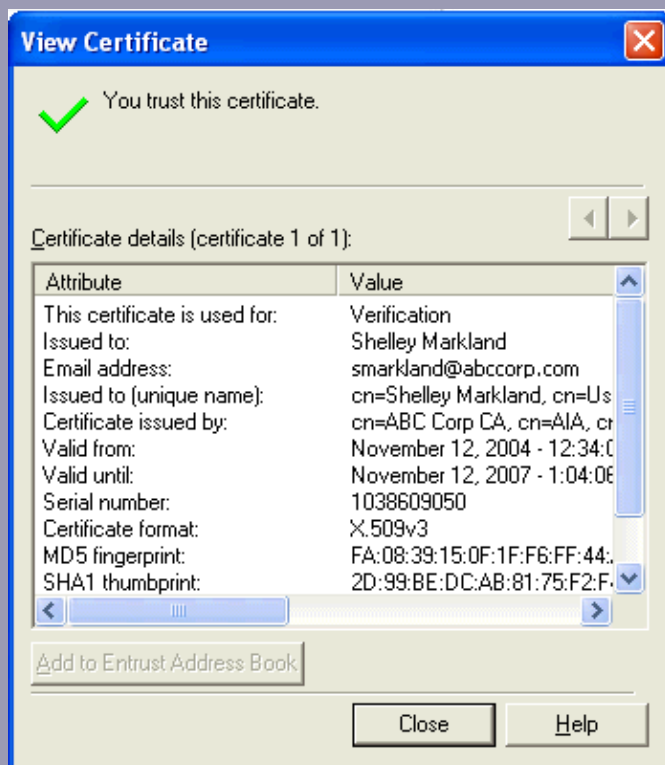
The Entrust Login can be located in the

- » Start Menu
- » All Programs
- » Entrust
- » Entrust Login



What is a Digital Signature?

Provides a guarantee to a recipient that the signed file indeed came from the person who sent it. It also guarantees that it was not altered since it was signed.



Certificate details identifying your authenticity...



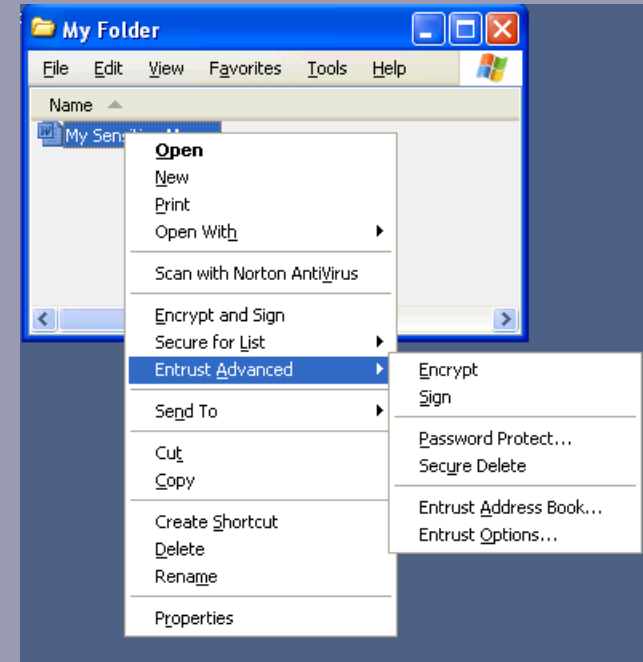
File Encryption Using Right Click Menu

Encrypt and Sign » encrypt and sign in one step

Secure for List » Select recipients

Entrust Advanced

- Encrypt » encrypt only
- Sign » sign only
- Password Protect » set password
- Secure Delete » encrypts file and moves to the Recycle Bin
- Entrust Address Book » opens the address book
- Entrust Options



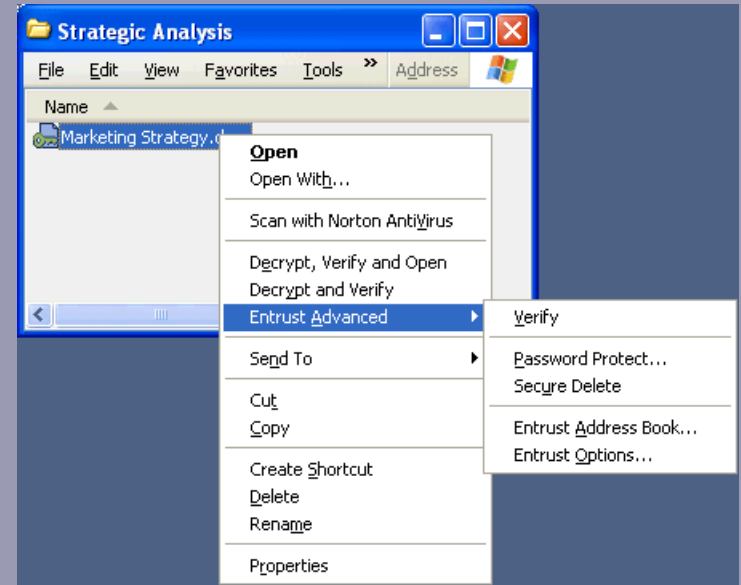
Removing Security Using the Right-Click Menu

Decrypt, Verify and Open »
decrypt, verify and open in one
step

Decrypt and Verify » decrypt and
verify only

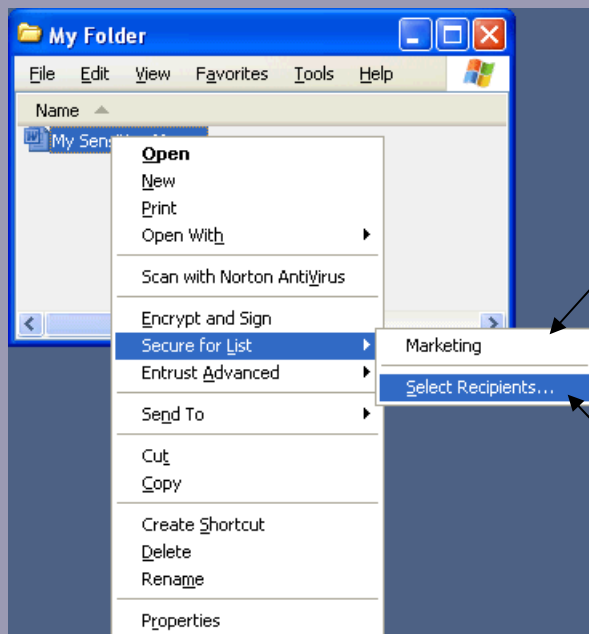
Entrust Advanced

- Verify » verifies the digital
signature is authentic
- Password Protect » set password
- Secure Delete » encrypts file and
moves to the Recycle Bin
- Entrust Address Book » open the
address book
- Entrust Options



Securing Files for Selected Recipients

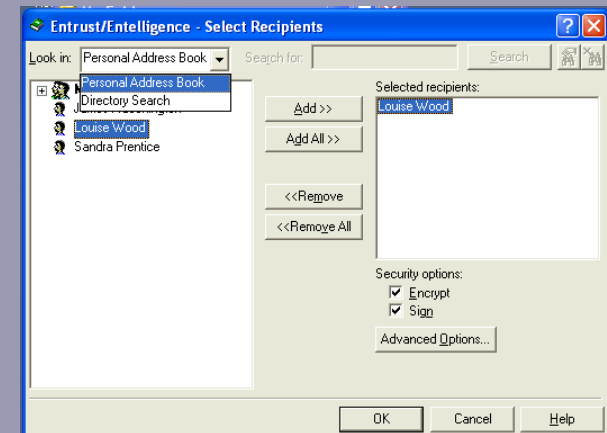
If you encrypt a file for yourself, only you will be able to decrypt it. If you want to secure a file for others, you need to specify your intended recipients. The intended recipient must also have a PKI Certificate.



Customized Recipient Lists will show in the menu

Right click on the document to choose Select Recipients

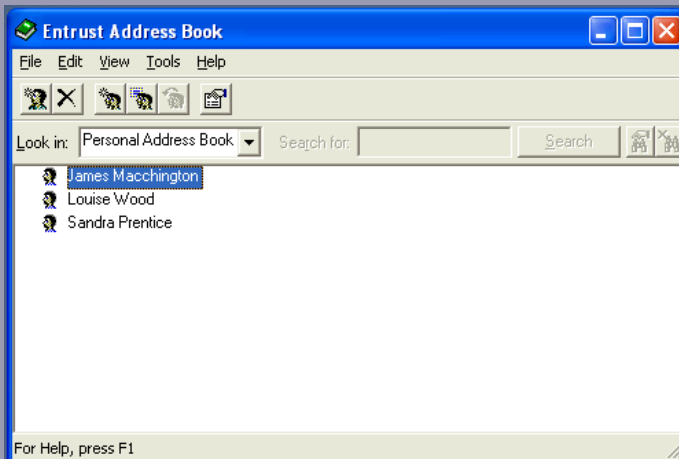
Select the intended recipients



Entrust Address Book

Instead of selecting individual recipients and specifying options when you secure a file, you can save a group of recipients in a list and specify options for the entire group.

To access the Entrust Address Book
Right click the Entrust key in your
Windows taskbar (next to the clock).



The Entrust Address Book is your link to the certificates stored in the Entrust Directory.

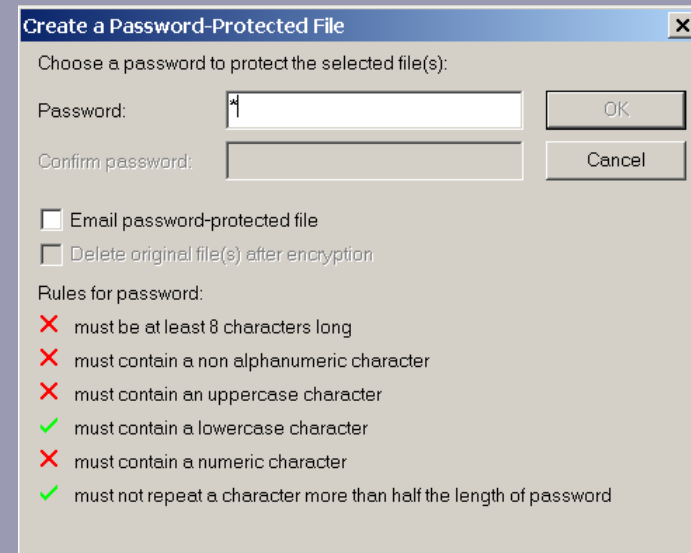
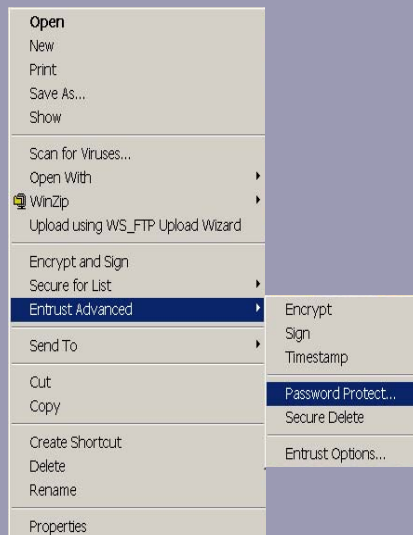
Through the address book you can create, view, and edit recipient lists, and view their properties.

Password Protect and Encrypt

Password protect and encrypt files for people who do not have security software installed on their computer.

It is recommended that the password is supplied to the recipient separate from the file.

Right-Click on the file/Choose Entrust Advanced/Password Protect



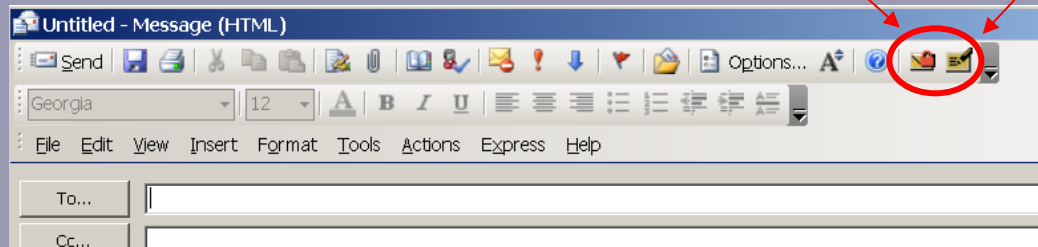
Securing E-mail with Entrust



Files can be encrypted and then attached to an email (the recipient must be identified when the file is encrypted) OR Attach an unencrypted file and then encrypt the email message.

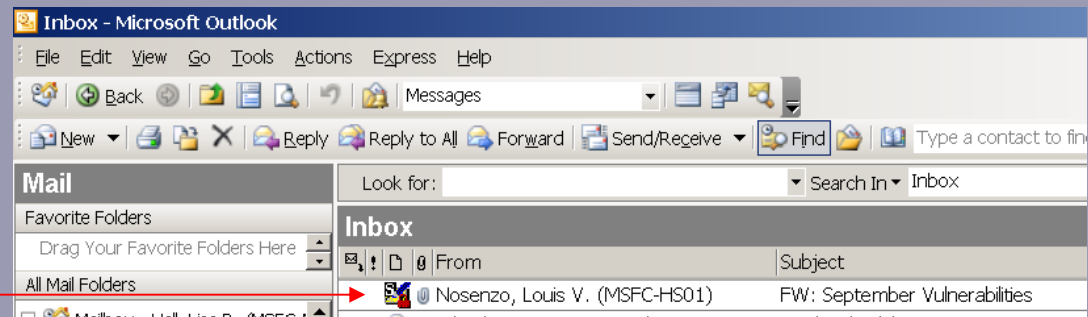
Please Note: The email recipient must have an Entrust certificate or the message will not be sent.

Prepare a new email message and select the Encryption button or the Digital Signature button or both.



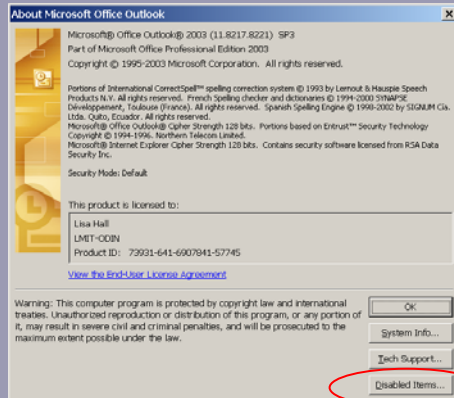
If these buttons are not showing on your new email message toolbar, see next slide for a resolution.

Encrypted messages received in your Inbox will be identified by this encryption icon.



Toolbar Buttons for Encryption & Digital Signature

On the Outlook menu select Help/About Microsoft Office Outlook



Select the Disabled Items button

On the Disable Items pop-up window.

Select the item from the list and click the Enable button.

NOTE: Microsoft Word cannot be set as your email editor.

This setting can be changed by going to the Outlook menu and selecting Tools/Options/Mail Format Tab

Using PKI with Entourage or Blackberries

These devices are able to use NASA issued certificates to operate more securely, but need to have access to your private key.

PKCS#12 allows the user to securely move their keys or certificates to those applications or devices.

For more info and access to the agreement go to:

<http://pki.nasa.gov/index.php/tech-support/pkcs12/>

The signed form is to be submitted to the MSFC Registration Authority in Bldg. 4312 or the 4200 Security desk (attn Kimberly or Terry).



How can I get PKI?

PKI Registration– 4 step process

(all steps must be completed within 30 days after receiving email from step 1)

1. Complete PKI certificate form (NF1773 – FileNet eForm version) and email to MSFC-PKIRA@mail.nasa.gov.
2. Pick-up authorization code after email notification (2 forms of ID are required along with original signed form 1773)
3. Entrust PKI software is part of the ODIN standard load.
4. Create your Entrust Profile using the instructions provided with your authorization code.

Computer based training is available at:

<http://pki.nasa.gov/index.php/personal-certificates/pki-training/>

A training course is also available in SATERN for NASA PKI. It may vary slightly from the PKI implemented at Marshall

PKI Recovery - contact Kimberly Rutkowski or Terry Mullen at 544-2090 or by email at MSFC-PKIRA@mail.nasa.gov